1   CLAIMS

2

3   1.   Apparatus, including

4   a storage element including an input disposed for receiving digital content

5 from a physical medium, the storage element being capable of non-evanescently storing

6 that digital content using a storage technique substantially different from the physical me-

7 dium;

8   a playback device coupled to the storage element, the playback device having

9 an input disposed for receiving the digital content and having an output disposed for cou-

10 pling a media stream represented by that digital content for presentation; and

11   including a media reader, the media reader having a read element capable of

12 being coupled to the physical medium.

13

14   2.   Apparatus as in claim 1, wherein the output for presentation includes a

15 signal following standards for protected signals specified by the CSS license.

16

17   3.   Apparatus as in claim 1, whereby the playback device includes a CSS

18 descrambler.

19

20   4.   Apparatus as in claim 1, whereby the playback device incorporates and

21 implements the functionalities of Disc Key Recovery Logic, Title Key Recovery Logic, and

22 the Content Scrambling Algorithm, and incorporates the Master Key pair.

23

24

1   5.   Apparatus as in claim 1, whereby the playback device does not incorpo-

2   rate or implement the functionality of the CSS Authentication Algorithm, or incorporate the

3   Authentication Key.

4

5   6.   Apparatus as in claim 1, whereby the media reader does not incorpo-

6   rates or implement the functionalities of any of Disc Key Recovery Logic, Title Key Recovery

7   Logic, or the Content Scrambling Algorithm, or incorporate the Master Key pair.

8

9   7.   Apparatus as in claim 1, whereby the media reader incorporates and

10   implements the functionality of the CSS Authentication Algorithm, and incorporates the

11   Authentication Key.

12

13   8.   Apparatus as in claim 1, whereby the media reader is or contains an Au-

14   thenticator for CSS Decryption Module and the playback device is or contains a Descram-

15   bler, such terms as defined in the CSS Procedural Specifications.

16

17   9.   Apparatus as in claim 1, whereby, when each media reader boots, it ob-

18   tains its operating software from the storage element.

19

20   10.   Apparatus as in claim 1, whereby any operating software for a compo-

21   nent of the apparatus, which is stored in the storage element, is encrypted when stored and

22   transmitted between components, and decrypted and authenticated in the component for

23   which it is such operating software, before said component becomes operative.

24

1   11.   Apparatus as in claim 1, whereby, when each playback device boots, it

2   obtains its operating software from the storage element.

3

4   12.   Apparatus as in claim 1, whereby the operating software for the media

5   reader, the storage element, and the playback device is not based on a general-purpose op-

6   erating system such as Microsoft Windows, or Linux, or a version of Unix.

7

8   13.   Apparatus as in claim 1, whereby the structure and operation of the file

9   system in the storage element is a trade secret.

10

11   14.   Apparatus as in claim 1, wherein the main printed circuit board of the

12   playback device has at least five layers, and signals containing unscrambled compressed

13   audiovisual data or key material run wherever feasible on traces in interior layers of the

14   board.

15

16   15.   Apparatus as in claim 1, wherein those integrated circuits in the play-

17   back devices signals containing unscrambled compressed audiovisual data or key material

18   run are area-array and such signals run wherever feasible on interior contacts of such inte-

19   grated circuits, and wherein those integrated circuits are surface-mounted.

20

21   16.   Apparatus as in claim 1, whereby the user can only interact with the

22   apparatus through either an on-screen display and associated touchpad and IR remote con-

23   trol protocols, or through a Web user interface.

24

1   17.   Apparatus as in claim 1, whereby, the audio data output from the play-

2 back device is either in a compressed format or else in a Linear PCM format in which the

3 transmission information is sampled at no more than 48 kHz and no more than 16 bits.

4

5   18.   Apparatus as in claim 1, whereby, the analog video data output from

6 the playback device does not have higher resolution than standard definition, unless the

7 content recorded on the physical medium has itself that higher resolution.

8

9   19.   Apparatus as in claim 1, wherein the playback device includes a plural-

10 ity of those outputs disposed for presentation, at least two of those outputs pairwise having

11 more than one controlling CPU and at least one of the properties in the set: being logically

12 remote, being physically remote.

13

14   20.   Apparatus as in claim 1, wherein the playback device includes at least

15 one of those outputs disposed for presentation having a distinct controlling CPU from the

16 storage element and having at least one of the properties in the set: being logically remote

17 from the storage element, being physically remote from the storage element.

18

19   21.   Apparatus as in claim 1, the digital content being maintained in a pro-

20 tected form

21   between the physical medium and the media reader,

22   between the media reader and the storage element,

23   when maintained on the storage element, and

24   between the storage element and the playback device.

1

2   22.   Apparatus as in claim 21, wherein

3   at least two elements in the set: the storage element, the playback device, the

4 media reader;

5   have, pairwise, at least two of the properties in the set: being logically remote,

6 being physically remote, having more than one controlling CPU.

7

8   23.   Apparatus as in claim 21, wherein

9   at least two elements in the set: the storage element, the playback device, the

10 media reader;

11   are pairwise physically remote, and have separate controlling CPUs.

12

13   24.   Apparatus as in claim 1, wherein the media reader includes at least one

14 DVD reader.

15

16   25.   Apparatus as in claim 1, wherein the media reader includes a DVD

17 drive and the physical media includes at least one DVD.

18

19   26.   Apparatus as in claim 1, wherein the storage element includes an array

20 of magnetic disk drives wherein data is stored redundantly in such a way that all data may

21 be recovered after the failure of any one disk drive therein.

22

23   27.   Apparatus as in claim 1, wherein the digital content is maintained in a

24 protected form for at least two cases in the set:

1   between the physical medium and the media reader;

2   between the media reader and the storage element;

3   when maintained on the storage element;

4   between the storage element and the playback device.

5

6   28.   Apparatus as in claim 1, wherein the digital content is maintained in a

7   protected form for at least three cases in the set:

8   between the physical medium and the media reader;

9   between the media reader and the storage element;

10   when maintained on the storage element;

11   between the storage element and the playback device.

12

13   29.   Apparatus as in claim 21, wherein the protected form includes at least

14   two of:

15   an encrypted form of the digital content;

16   an encrypted form of the digital content complying with the CSS license;

17   a form of the digital content including digital rights information;

18   a form of the digital content including digital rights information for which it

19   is substantially difficult to remove that digital rights information.

20

21   30.   Apparatus as in claim 21, wherein the protected form has at least one of

22   the properties in the set:

23   resistant to attempts to defeat copy protection afforded by the protected form,

24   impossible to defeat using user tools,

1   difficult to defeat using professional tools.

2

3   31.   Apparatus as in claim 21, wherein the protected form has at least two of

4   the properties in the set:

5   resistant to attempts to defeat copy protection afforded by the protected form,

6   impossible to defeat using user tools,

7   difficult to defeat using professional tools.

8

9   32.   Apparatus as in claim 21, wherein the protected form is substantially

10   resistant to attempts to defeat copy protection afforded by the protected form, is substan-

11   tially impossible to defeat using user tools, and is substantially difficult to defeat using pro-

12   fessional tools.

13

14   33.   Apparatus as in claim 1, wherein the media reader includes a first au-

15   thenticator and the system exclusive of the media reader includes a second authenticator.

16

17   34.   Apparatus as in claim 33, wherein the system complies with CSS proce-

18   dures.

19

20   35.   Apparatus as in claim 33, wherein the system is capable of having the

21   first authenticator and the second authenticator authenticate each other before the media

22   reader permits access to data.

23

24   36.   Apparatus as in claim 33, wherein the system is capable of

1   using CSS descrambling procedures at the playback device.

2

3   37.   Apparatus as in claim 1, wherein the storage element has capacity to

4   concurrently store digital content from plural physical media.

5

6   38.   Apparatus as in any of claims 1 or 20 or 21 or 32 or 33, wherein opera-

7   tion of the system includes at least a substantial time duration between a first time of stor-

8   age of the digital content at the storage element, and a second time of output of any media

9   stream derived in response thereto.

10

11   39.   Apparatus as in any of claims 1 or 20 or 21 or 32 or 33, wherein the

12   digital content is transported any substantial distance after being read by the media reader

13   and before being output by the playback device.

14

15   40.   Apparatus as in any of claims 1 or 20 or 21 or 32 or 33, including at

16   least one system internal link, the at least one system internal link including a link able to

17   communicate compressed digital data representing media streams;

18   wherein at least one of the following communicated using the system internal

19   link is not substantially accessible to an external entity without an authorized cryptographi-

20   cally secure key: digital information representing at least one media stream, digital rights

21   information, digital rights key information.

22

1   41.   Apparatus as in claim 40, including steps of coupling by a least one sys-

2   tem internal link, at least two of the set: the media reader, the storage element, the playback

3   device.

4

5   42.   A media reader, including

6   a read element for physical media, the physical media including digital con-

7   tent representing at least one media stream, the digital content being maintained in a pro-

8   tected form, and the read element including a first authenticator;

9   a second authenticator;

10   an interface to a storage element; and

11   a controller capable of (1) causing the first authenticator and the second au-

12   thenticator to authenticate each other before the read element accesses the physical media,

13   and (2) causing the read element to read data from the physical media and output the data

14   to the interface with DRM information intact.

15

16   43.   A media reader as in claim 42, wherein the read element includes a

17   DVD drive.

18

19   44.   A media reader as in claim 42, wherein the media reader can output the

20   data to the storage element whether or not the storage element is logically remote from the

21   media reader.

22

23   45.   A method of playing media, including steps of

1   reading physical media including digital content representing at least one me-

2   dia stream, the digital content being maintained in a protected form;

3   non-evanescently storing the digital content in the protected form using a

4   storage mechanism different from the physical media; and

5   playing back the digital content after conversion into analog, digital, or analog

6   and digital audiovisual content in a second protected from for presentation.

7

8   46.   A method as in claim 45, wherein additional protection is used on the

9   physical media, by the storage mechanism, or both.

10

11   47.   A method as in claim 46, wherein the additional protection used on the

12   physical media is different from the additional protection used by the storage mechanism.

13

14   48.   A method as in claim 45, wherein the protected form complies with CSS

15   procedures.

16

17   49.   A method as in claim 48, whereby the step of playing back incorporates

18   and implements the functionalities of Disc Key Recovery Logic, Title Key Recovery Logic,

19   and the Content Scrambling Algorithm, and involves the Master Key pair.

20

21   50.   A method as in claim 48, whereby the step of playing back does not in-

22   corporate or implement the functionality of the CSS Authentication Algorithm, or incorpo-

23   rate the Authentication Key.

24

1   51.   A method as in claim 48, whereby the step of reading does not incorpo-

2   rate or implement the functionalities of any of Disc Key Recovery Logic, Title Key Recovery

3   Logic, or the Content Scrambling Algorithm, or incorporate the Master Key pair.

4

5   52.   A method as in claim 48, whereby the step of reading incorporates and

6   implements the functionality of the CSS Authentication Algorithm, and involves the Au-

7   thentication Key.

8

9   53.   A method as in claim 48, whereby

10   the step of reading performs the function of an Authenticator for CSS Decryp-

11   tion Module; and

12   the step of playing back peforms the function of a Descrambler;

13   as those terms defined in the CSS Procedural Specifications.

14

15   54.   A method as in claim 48, whereby, when the step of reading begins, it

16   includes the step of obtaining software from the storage element.

17

18   55.   A method as in claim 48, whereby, when the step of playing back be-

19   gins, it includes the step of obtaining software from the storage element.

20

21   56.   A method as in claim 55, whereby the operating software for the step of

22   reading, the storage element, and the step of playing back is not based on a general-purpose

23   operating system such as Microsoft Windows, or Linux, or a version of Unix.

24

1   57.   A method as in claim 48, whereby, the audio data output from the step

2   of playing back is either in a compressed format or else in a Linear PCM format in which the

3   transmission information is sampled at no more than 48 kHz and no more than 16 bits.

4

5   58.   A method as in claim 48, whereby, the analog video data output from

6   the step of playing back does not have higher resolution than standard definition, unless the

7   content recorded on the physical medium has itself that higher resolution.

8

9   59.   A method as in claim 45, wherein the protected form includes at least

10   two of:

11   an encrypted form of the digital content;

12   an encrypted form of the digital content complying with the CSS license;

13   a form of the digital content including digital rights information;

14   a form of the digital content including digital rights information for which it

15   is substantially difficult to remove that digital rights information.

16

17   60.   A method as in claim 45, wherein the protected form includes

18   an encrypted form of the digital content complying with the CSS license; and

19   an additional layer of protection, by any technique, for any substantial portion

20   of the steps of reading, storing, and playing back.

21

22   61.   A method as in claim 45, wherein the physical media includes at least

23   one DVD and the step of reading occurs in at least one DVD drive in a media reader.

24

1   62.   A method as in claim 45, wherein

2   the physical media includes at least one high-definition optical disc, in at least

3   one of the following formats: Blu-Ray, HD-DVD, another format requiring a blue laser; and

4   the step of reading that optical disc in a media reader includes a blue laser.

5

6   63.   A method as in claim 61, wherein the media reader includes a first au-

7   thenticator.

8

9   64.   A method as in claim 63, wherein the method complies with CSS pro-

10   cedures.

11

12   65.   A method as in claim 64, wherein part of complying with said CSS pro-

13   cedures includes having the first authenticator and a second authenticator authenticate

14   each other before permitting access to data.

15

16   66.   A method as in claim 64, wherein part of complying with said CSS pro-

17   cedures includes using CSS descrambling procedures.

18

19   67.   A method as in claim 64, wherein part of complying with said CSS pro-

20   cedures includes extracting keys that can be used to descramble CSS data, by an indirect

21   manner from the key materials copied from the optical disc, using a key associated with the

22   playback device, that key not being available from the optical disc.

23

1   68.   A method as in claim 64, wherein part of complying with said CSS pro-

2   cedures includes having the first authenticator and the second authenticator authenticate

3   each other before the media reader permits access to data, and using CSS descrambling pro-

4   cedures.

5

6   69.   A method as in claim 45, wherein at least two of the following steps oc-

7   cur at logically remote locations: the step of reading, the step of non-evanescently storing,

8   and the step of playing back.

9

10   70.   A method as in claim 45, wherein at least two of the following steps oc-

11   cur at physically remote locations: the step of reading, the step of non-evanescently storing,

12   and the step of playing back.

13

14   71.   A method as in claim 45, wherein the step of playing back occurs at a

15   plurality of playback devices, at least two of those playback devices being pairwise substan-

16   tially physically remote from each other.

17

18   72.   A method as in claim 45, wherein a substantial time duration occurs

19   between the step of non-evanescently storing and the step of playing back.

20

21   73.   A method as in claim 74, wherein the digital content is transported any

22   substantial distance between the step of reading and the step of playing back.

23

1   74.   A method as in claim 45, wherein the digital content is transported any

2   substantial distance between the step of reading and the step of playing back.

3

4   75.   A method as in claim 45, wherein at least one system internal link is

5   used between two of the steps of reading, non-evanescently storing, and playing back, the at

6   least one system internal link including a link able to communicate compressed digital data

7   representing media streams but which need not be substantially able to effectively and

8   timely communicate uncompressed digital data representing media streams; and

9   wherein any key materials in data communicated using the system internal

10   link is not substantially accessible to an external entity without an authorized cryptographi-

11   cally secure key.

12

13   76.   A method of doing business, including steps of sending data from a de-

14   vice that reads a physical medium to a remote playback device while complying with CSS li-

15   cense agreement terms and CSS procedural specification terms.

16

17   77.   A method of doing business as in claim 76, wherein the steps of sending

18   data to a remote playback device include causing that playback device to be ready to play-

19   back that data.

20

21   78.   A method of doing business as in claim 76, wherein the physical me-

22   dium is a DVD.

23

1   79.   A method of doing business as in claim 76, wherein the device that

2   reads the physical medium and the remote playback device have separate controlling CPUs,

3   and have at least one of the properties in the set: being logically remote, being physically

4   remote.

5

6   80.   A method of doing business as in claim 76, including steps of storing

7   data from the physical medium in a storage element capable of non-evanescently storing

8   that digital content using a storage technique substantially different from the physical me-

9   dium.

10

11   81.   A method of doing business as in claim 76, including steps of storing

12   data from the physical medium in a storage element capable of non-evanescently storing

13   that digital content using a storage technique substantially different from the physical me-

14   dium; and

15   wherein the playback device is coupled to the storage element, the playback

16   device having an input disposed for receiving the digital content and having an output dis-

17   posed for coupling a media stream represented by that digital content for presentation.

18

19   82.   A method of doing business as in claim 81, whereby the playback device

20   includes a CSS descrambler.

21

22   83.   A method of doing business as in claim 81, wherein the playback device

23   includes a plurality of those outputs disposed for presentation, at least two of those outputs

1   pairwise have separate controlling CPUs, and have at least one of the properties in the set:

2   being logically remote, being physically remote.

3

4   84.   A method of doing business as in claim 81, wherein the playback device

5   includes at least one of those outputs disposed for presentation and having at least one of

6   the properties in the set: being logically remote from the storage element, being physically

7   remote from the storage element, having a distinct controlling CPU from the storage ele-

8   ment.

9

10   85.   A method of doing business as in claim 81, wherein data is read from

11   the physical medium by a media player before being sent to the storage element, and

12   wherein the media reader includes a read element capable of being coupled to the physical

13   medium, the digital content being maintained in a protected form between the media reader

14   and at least one of: the storage element, the playback device.

15

16   86.   A method of doing business as in claim 85, wherein

17   at least two elements in the set: the storage element, the playback device, the

18   media reader;

19   have collectively more than one controlling CPU, and have pairwise, at least

20   one of the properties in the set: being logically remote, being physically remote.

21

22   87.   A method of doing business as in claim 85, wherein the digital content

23   is maintained in a protected form for substantially an entire path including:

24   between the physical medium and the media reader;

1   between the media reader and the storage element;

2   when maintained on the storage element;

3   between the storage element and the playback device.

4

5   88.   A method of doing business as in claim 85, wherein the protected form

6   includes at least two of:

7   an encrypted form of the digital content;

8   an encrypted form of the digital content complying with the CSS license;

9   a form of the digital content including digital rights information;

10   a form of the digital content including digital rights information for which it is

11   substantially difficult to remove that digital rights information.

12

13   89.   A method of doing business as in claim 85, wherein the protected form

14   has at least one of the properties in the set:

15   resistant to attempts to defeat copy protection afforded by the protected form,

16   impossible to defeat using user tools,

17   difficult to defeat using professional tools.

18

19   90.   A method of doing business as in claim 85, wherein the protected form

20   has at least two of the properties in the set:

21   resistant to attempts to defeat copy protection afforded by the protected form,

22   impossible to defeat using user tools,

23   difficult to defeat using professional tools.

24

1   91.   A method of doing business as in claim 85, wherein the protected form

2   is substantially resistant to attempts to defeat copy protection afforded by the protected

3   form, is substantially impossible to defeat using user tools, and is substantially difficult to

4   defeat using professional tools.

5

6   92.   A method of doing business as in claim 81, wherein the storage element

7   has capacity to concurrently store digital content from plural physical media.

8

9   93.   A method of doing business as in claim 81, wherein

10   at least one possible output from the playback device includes an analog

11 audiovisual content; and

12   the second protected form by which the analog audiovisual content is pro-

13 tected includes analog copy protection.

14

15   94.   A method of doing business as in claim 93, wherein the analog copy

16 protection is Macrovision copy protection.

17

18   95.   A method of doing business as in claim 81, wherein

19   at least one output from the playback device includes a digital audiovisual

20 content; and

21   the second protected form by which the digital audiovisual content is pro-

22 tected includes a technique substantially like HDCP.

23

1   96.   A method of doing business as in claim 81, wherein operation of the

2 system includes at least a substantial time duration between a first time of storage of the

3 digital content at the storage element, and a second time of output of any media stream de-

4 rived in response thereto.

5

6   97.   A method of doing business as in claim 81, wherein the digital content

7 is transported any substantial distance after being read by the media reader and before be-

8 ing output by the playback device.

9

10   98.   A method of doing business as in claim 81, including at least one sys-

11 tem internal link, the at least one system internal link including a link able to communicate

12 compressed digital data representing media streams;

13   wherein at least one of the following communicated using the system internal

14 link is not substantially accessible to an external entity without an authorized cryptographi-

15 cally secure key: digital information representing at least one media stream, DRM informa-

16 tion, DRM key information.

17

18   99.   A method of doing business as in claim 98, including steps of coupling

19 by a least one system internal link, at least two of the set: the media reader, the storage ele-

20 ment, the playback device.

21

22   100.   A method of doing business as in claim 81, wherein data is read from

23 the physical medium by a media player before being sent to the storage element, and

24 wherein the media reader includes

EL 768 962 880 US   48

1   a read element for physical media, the physical media including digital con-

2   tent representing at least one media stream, the digital content being maintained in a pro-

3   tected form, and the read element including a first authenticator;

4   a second authenticator;

5   an interface to a storage element; and

6   a controller capable of (1) causing the first authenticator and the second au-

7   thenticator to authenticate each other before the read element accesses the physical media,

8   and (2) causing the read element to read data from the physical media and output the data

9   to the interface with DRM information intact.

10

11   101.   A method of doing business as in claim 100, wherein the read element

12   includes a DVD drive.

13

14   102.   A method of doing business as in claim 100, wherein the media reader

15   can output the data to the storage element whether or not the storage element is logically

16   remote from the media reader.